UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/541,934 | 01/26/2007 | Jesus-Angel de Gregorio | P17270-US1 | 6753 |

27045 7590 06/16/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

| EXAMINER | |
|---|---|
| KELLEY, STEVEN SHAUN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2617 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 06/16/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/541,934 | DE GREGORIO ET AL. | |
| | Examiner | Art Unit | |
| | STEVEN KELLEY | 2617 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *01 March 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-14 and 19 are rejected under 35 U.S.C. 103(a) as obvious over WO 02/011467 to Jones et al. (hereinafter "Jones") in view of U.S. Pat. Pub. No. 2003/0051041 to Kalavade et al. (hereinafter "Kalavade") and the Liberty Alliance Project (LAP) Specifications documents published July 11, 2002 (entitled "Liberty Alliance Overview" and "Liberty Bindings and Profiles Specification").

Regarding the structures recited in claim 1, Jones teaches a visited Serving GPRS Node 27 (included in an Integrated Network Controller 24), which is connected to a Roaming RADIUS Server 37 and a Home RADIUS server 34, which are connected and function as recited in claim 1. See for example, Figs. 1 and 4, the description thereof. Although Jones teaches that the visited AAA (RADIUS) server 37 communicates with the home AAA server 34, Jones does not explicitly disclose that the visiting AAA server "binds the home AAA server address with the user's identifiers." In an analogous art, Kalavade teaches a system for consolidated billing used with roaming wireless devices, see for example, Fig. 1 of Kalavade. Kalavade teaches that a user may enter a phone number and password via a Converged Billing /Authentication

Gateway (CBG) server 10 (which reads on the recited "global Single Sign-On Front End infrastructure") in order to access services in a home network. Kalavade also includes a CBG database 14 used to store information relating to a roaming user and related information. Kalavade shows (on pages 11-13) the details of the information stored relating to a roaming user, which include IP addresses of WLAN endpoints, such as for example, a home billing system or HLR, etc. Therefore, in order to increase the efficiency of billing procedures and communications, it would have been obvious to modify the visited AAA server of Jones to include the capability of binding a user's identifiers with a home AAA server as taught by Kalavade.

Additionally, regarding the recited "GGSN", although the Integrated Network Controller (INC 24) of Jones includes two devices, a radio network controller (RNC 26) and a Serving GPRS Support Node (SGSN 27), a GGSN is not explicitly shown as being included in the INC 24. Kalavade teaches in section [0006] that GGSNs are used to attach to core networks and sections [0218] to [0219] (which described the GGSN 62 and SGSN 60 in Fig. 11) show using both an SGSN and a GGSN for network connections and billing purposes. Additionally, as set forth on page 9 of Applicant's arguments (citing the 3GPP TS 23.060 Standards Document from 2002) it is conventional and well known that "The SGSN and the GGSN functionalities may be combined in the same physical node". Therefore, as Jones teaches integrating multiple devices (the RNC 26 and SGSN 27) into the INC 24, and it is well known that SGSNs and GGSNs may be integrated within the same physical node, it would have been

obvious to one of ordinary skill to include a GGSN (as in Kalavade) into the INC 24 of Jones, as is conventional.

Regarding the features of claim 1, which recite "a number of Service Providers that have signed service agreements with the Multinational Mobile Network Operator federation for offering Single Sign-On services to users that are subscribers of any National Network Operator included in the federation, each Service Provider in the federation providing a specific Uniform Resource Identifier (URI), as physical SSO entry point towards the federation, and each Service Provider comprising: redirection means for redirecting the user to the global Single Sign-On Front End (G-SSO-FE) as entry point in the federation; receiving means for receiving a token from the user along with an indication of where the token was generated; retrieval means for retrieving an authentication assertion from a site where the token was generated; and checking means for checking that such site is trusted", although Jones teaches (on page 11) of using a network access identifier such as "user@realm" and identifying one of a number of service providers and Kalavade teaches transmitting/receiving authentication tokens (see sections [0089]-[0090] and [0160]-[0176]), the Liberty Alliance Project documents which describe structures and processes of "a number of Service Providers that have signed service agreements with the Multinational Mobile Network Operator federation for providing SSO services" are added to show the above recited features.

Regarding the above features (which are recited as being included in each service provider), see for example pages 11-22 and 30-32 of the Liberty Bindings and Profiles Specification, which teach (and show in Figs. 1-3) using a URL such as a

"Single Sign On Service URL" or an "Assertion Consumer Service URL", which reads on the recited "each Service Provider in the federation providing a specific Uniform Resource Identifier (URI), as physical SSO entry point towards the federation". Regarding the recited "redirection means", "receiving means", "retrieval means" and "checking means" (which are included in a service provider), see the "Service Provider" shown in Figure 1. See for example pages 11-22 and 30-32 of the Liberty Bindings and Profiles Specification, which describe examples (as shown in Figs. 1-3 and 7) of SSO processes. The processes described involve numerous steps of transmitting and receiving SSO assertion data (which are the recited "redirecting, receiving, retrieving and checking" included in the Service Provider shown in Figure 1) such as authentication requests and authentication responses between the user agent, the service provider and the identity provider, where the recited "token" is the information included in the authentication assertions and responses (such as the "artifact"). See also for example, pages 8-17 of the Liberty Architecture Overview document, which teach SSO examples which involve Authentication (section 3.2.2) and pages 18-19, which teach redirecting authentication requests and data between the user, the service provider and the identity provider.

Therefore, as Jones teaches the conventionality of transmitting/receiving user information between a number of service providers and Kalavade teaches transmitting/receiving user information and authentication tokens, it would have been obvious to one of ordinary skill in the art to modify the system of Jones/Kalavade to additionally provide the recited "means" included in each service provider (as described

in the LAP specification documents) in order to provide the user with SSO services via a number of different service providers, which enhances the user's experience logging into different service providers by avoiding user re-authentications (as taught by the LAP specifications documents).

Regarding claims 2-3, the CBG database 14 of Kalavade teaches the recited features of the "Global Directory". See also the LAP specifications documents which teach a "number of multinational network operators".

Regarding the information recited in claims 4-6, as described above, Kalavade shows on pages 11-13 the details stored in the CBG database, which include the recited IP addresses, user identifiers, passwords and time stamp recited in these claims.

Regarding claims 7-9, see the LAP specifications documents which teach "authentication assertions" as in claim 7. Although Jones shows only one visited GPRS node 27 used to access a visited network, it is common for a plurality of networks to be connected, as taught in the LAP specifications documents. Kalavade teaches in section [0204] that each network and/or "hot spot" "typically has its own authentication infrastructure". Therefore it would have been obvious in view of the teachings of the LAP specification documents and Kalavade to modify Jones to include sign on infrastructure for each connected network and/or service provider, in order to allow roaming users to sign on to any available network.

Regarding claim 10, as described above, Jones teaches a system for authenticating roaming users. Figs. 3-5 of Jones shows the claimed steps of (a) authenticating a roaming user in a visited packet radio network, via a proxy (see page 9 lines 26-29 of Jones which teaches that "In decision step 3, the partner radius server 37 verifies user ID and password", where the visited partner radius server 37 "authenticates" and acts as a "proxy", as now recited) (b) creating a master session at the user's home service network (c) redirecting a user towards the user's home network and (d) receiving an authentication from the home server. Jones does not explicitly disclose that the master session created in the user's home network is created with "Single Sign-On related data, as recited in step (b). As described above, Kalavade teaches a system for consolidated billing used with roaming wireless devices where a user may enter a phone number and password via a Converged Billing /Authentication Gateway (CBG) server 10, in order to access services in a home network. Kalavade further teaches of forwarding "single sign on related data" such as the entered phone number, IMSI number and information as shown in the table on pages 11-13, to backend accounting and billing servers/systems. Therefore, in order to correctly track, identify and bill roaming users within a network, it would have been obvious to modify the home RADIUS server of Jones to include the capability of creating a master session with single sign on related data, as shown in Kalavade.

Regarding the amendments to claim 10, which now recite that "each service provider in the federation providing a specific Uniform Resource Identifier as the Single Sign-On service, receiving a Single Sign On authentication assertion from the user or

from an entity where such assertion was generated, along with an address of such entity and validating the Single Sign On authentication assertion with the entity having generated the assertion", although Jones does teach (on page 11) using a network access identifier such as "user@realm" and identifying one of a number of service providers and Kalavade teaches exchanging authentication token, the LAP specification documents are added for completeness.

Regarding the above features, see for example pages 11-22 and 30-32 of the Liberty Bindings and Profiles Specification, which teach (and show in Figs. 1-3 and 7) using a "Single Sign On Service URL" and an "Assertion Consumer Service URL", which read on the recited "each Service Provider in the federation providing a specific Uniform Resource Identifier (URI), as physical SSO entry point towards the federation". Regarding the recited "receiving an SSO assertion" and "validating the SSO assertion", see for example pages 11-22 and 30-32 of the Liberty Bindings and Profiles Specification, which describe examples (as shown in Figs. 1-3 and 7) of SSO processes. The processes described involve numerous steps of transmitting and receiving SSO assertion data (which are the recited "receiving and validating") such as authentication requests and authentication responses (which include digital signatures and artifacts used to validate) between the user, the service provider and the identity provider. Additionally, as the identity provider address is included in the information transmitted between devices in Figs. 1-3 and 7, the recited feature of "along with the address which generated the assertion", is included in the processes described in the LAP specification documents. See also for example, pages 8-17 of the Liberty

Architecture Overview document, which teach SSO examples which involve Authentication (section 3.2.2) and pages 18-19, which teach redirecting authentication requests and data between the user, the service provider and the identity provider.

Therefore, as Jones teaches the conventionality of transmitting/receiving user information between a number of service providers and Kalavade teaches transmitting/receiving user information and authentication tokens, it would have been obvious to one of ordinary skill in the art to modify the system of Jones/Kalavade to additionally provide the recited "URI" from each service provider (as described in the LAP specification documents) and to provide validation of the authentication assertions, in order to provide the user with SSO services via a number of different service providers, which enhances the user's experience logging into different service providers by avoiding user re-authentications (as taught by the LAP specifications documents).

Regarding claims 11 and 13, Kalavade shows a table on pages 11-13 that include the recited IP addresses, user identifiers, passwords and time stamp, recited in these claims.

Regarding claim 12, Kalavade teaches assigning a GRPS node to the user and transmitting the address of the GGSN used. See for example, Fig. 11 and information in the table on pages 11-13.

Regarding claim 14, Jones shows the visited AAA server 37, connected and acting as a proxy between the GPRS Support node and the home AAA server.

Regarding claim 19, Kalavade and the LAP documents teach providing addresses of devices (recited "entities") validating and authenticating user information.

6. Claims 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones, Kalavade and the LAP specifications documents as applied to claims 1-14 above, and further in view of U.S. Patent 6,578,085 to Khalil et at. (hereinafter "Khalil"). Claim 15 recites "determining the visited network which assigned the current IP address to the user". Khalil teaches tracking IP addresses assigned to a mobile node, where the IP addresses are assigned by a number of foreign networks. Khalil further teaches "determining visited networks which assigned IP addresses to a user", as shown in Figs. 10-13, which detail and describe the communications between the home and foreign networks regarding the registering and deregistering of IP addresses assigned to the mobile node by the foreign networks. Therefore, in order to correctly track, identify and bill roaming users within a number of networks, it would have been obvious to modify the Jones/Kalavade/LAP documents combination to include the capability of determining visited networks, as shown in Khalil.

### *Response to Arguments*

Applicant's arguments filed March 6, 2010 have been fully considered but they are not persuasive. The Examiner was persuaded by Applicant's arguments which

related to the fact that Jones did not explicitly teach a "GGSN". Regarding this feature, a new ground of rejection has been set forth above. As described in the rejection of claim 1, as Jones teaches integrating multiple devices (the RNC 26 and SGSN 27) into the INC 24, and it is well known that SGSNs and GGSNs may be integrated within the same physical node, it would have been obvious to one of ordinary skill to include a GGSN (as in Kalavade) into the INC 24 of Jones, as is conventional. Including the GGSN functionality within the INC 24 of Jones also addresses Applicant's statement on page 11 of the Remarks that "a skilled person would be in doubt where the GGSN missing in Jones could be located". Regarding Applicant's arguments on pages 11-12, which relate to the ambiguity of which/how elements in the LAP documents correspond to the claimed features, as the LAP documents are added to show the claimed elements "included within each service provider", Applicant's attention is directed to the "Service Provider" shown in Figure 1, as containing these recited elements. Specifically, on page 12, Figure 1 shows an 11 step process by which a user accesses the SSO system using a URL. These 11 steps are described in detail on pages 12-15. Regarding the recited "redirecting means", "receiving means", "retrieval means" and "checking means", these "means" are all included within the software components which perform the processes described in steps 1-11 *included in the Service Provider*. For example, regarding the recited "redirection means" see the description of steps 1-3, which repeatedly teach that the service provider "redirects" the flow of SSO authentication and assertion signals such as for example, "the *service provider* obtains the address of the appropriate identity provider to *redirect* the user agent to step 3". Regarding the

"receiving means", "retrieval means" and "checking means", these are also included in the Service Provider of Figure 1, as the authentication assertions and token are received (by the Service Provider) from the "user agent" and "identity provider" (recited "indication of where the token was generated" and "site where the token was generated"). See steps 1, 7 and 9, for example. Specifically, the authentication requests and authentication responses between the user agent, the service provider and the identity provider, include a "token", where the "token" is the information included in the authentication assertions and responses (such as the "artifact").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven Kelley whose telephone number is (571) 272-5652. The examiner can normally be reached on Monday-Friday, 9AM to 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on (571) 272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SSK

/LESTER KINCAID/

Supervisory Patent Examiner, Art Unit 2617